Joshua B. Swigart (WSBN 49422)
josh@swigartlawgroup.com
SWIGART LAW GROUP, APC
2221 Camino Del Rio S., Suite 308
San Diego, CA 92108
Tel: (866) 219-3343; Fax: (866) 219-8344

Akylah Cooper (WSBN 54108)
akylah@lawyerkevin.com
THE LAW OFFICE OF KEVIN LEMIEUX, APC
2221 Camino Del Rio S., Suite 308
San Diego, CA 92108
Tel: (619) 488-6767; Fax: (619) 488-6767

Attorneys for Plaintiff, JOHN DOE

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

JOHN DOE, Plaintiff, v. LASTPASS US LP, and DOES 1-10, Defendants.	Case No.: **COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff JOHN DOE ("Plaintiff"), by and through their attorneys, brings this action against Defendant LASTPASS US LP ("LastPass" or "Defendant"), and Defendants DOES 1-10. Plaintiff hereby alleges, on information and belief, except for information based on personal knowledge, which allegations are likely to have evidentiary support after further investigation and discovery, as follows:

INTRODUCTION

1. Plaintiff brings this action because of Defendant's failure to properly secure and safeguard Plaintiff's highly sensitive consumer data which resulted in the unauthorized public release, subsequent misuse, and theft of digital assets. On at least two (2) occasions and spanning for months, Defendant failed to exercise reasonable care in securing and safeguarding millions of LastPass users' highly sensitive consumer data in the data breach ("Data Breach"). The highly sensitive consumer data includes name, end-user name, billing addresses, email addresses, telephone numbers, IP addresses from which LastPass customers access the LastPass service, and customer vault data of stored, unencrypted data, which includes website usernames and passwords, secure notes, IP addresses, billing details, and form-filled data (collectively, "Sensitive Information"). Due to the misuse of Plaintiff's Sensitive Information, over $200,000 of Plaintiff's cryptocurrency was stolen.

2. Defendant is a global password and identity management solutions company used by million of users and over 100,000 businesses worldwide. Defendant boasts that it is "*a pioneer in cloud security technology*." Its site points to how data breaches are on the rise due to inadequate password security, then states that "*LastPass provides award-winning password and identity management solutions that are convenient, effortless, and easy to manage.*" It also states that *"LastPass values users' privacy and security, so your sensitive information is always hidden – even from us*."[1] Defendant also promotes its services of 24/7 dark web monitoring and proactive protection.[2]

3. Plaintiff subscribed to Defendant's password management service to securely store personal and financial login credentials, including those for cryptocurrency accounts.

4. Plaintiff stored cryptocurrency wallet credentials, including private keys and seed

[1]About LastPass, LastPass, (January 28, 2025), https://www.lastpass.com/company/about-us.
[2] Dark web monitoring, LastPass (January 28, 2025), https://www.lastpass.com/features/dark-web-monitoring.

phrases, within their LastPass vault.

5. Defendant boasts to its customers that it used industry-leading encryption and security protocols to protect user data.

6. Reasonably so, Plaintiff relied on and entrusted Defendant to safeguard their Sensitive Information, including prevention of their Sensitive Information being disseminated on the dark web for the hands of thieves to misuse.

7. In August of 2022, Defendant suffered an unauthorized data breach, and its attacker obtained portions of the company's source code and proprietary technical information.

8. In November to December of 2022, attackers used said proprietary information obtained in the August 2022 breach to access customers' Sensitive Information (i.e., encrypted customer vault backups and unencrypted metadata).

9. Plaintiff had a right to keep their Sensitive Information provided to Defendant confidential. Plaintiff relied on Defendant to keep their Sensitive Information confidential as required by the applicable laws.

10. Defendant violated this right. It failed to implement or follow reasonable data security procedures as required by law and failed to protect Plaintiff's Sensitive Information from unauthorized access and subsequent misuse.

11. As a result of Defendant's inadequate data security and inadequate or negligent training of its employees, Plaintiff's Sensitive Information was made available on the dark web in the Data Breach.

12. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiff's Sensitive Information.

13. Defendant disregarded the rights of Plaintiff by, among other things, recklessly or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have reasonable or adequately robust computer systems and security practices to safeguard Plaintiff's Sensitive Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely

detect the Data Breach; and failing to provide Plaintiff prompt and accurate notice of the Data Breach.

14. As a result of Defendant's failure to implement and follow reasonable security procedures, Plaintiff's Sensitive Information is now exposed. Following the Data Breach, on or about February 19, 2024, unauthorized actors accessed Plaintiff's LastPass vault and stole cryptocurrency assets worth over $200,000.

15. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's Sensitive Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's Sensitive Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

16. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect member data.

17. Defendant could have prevented the intrusions into its systems and, ultimately, the theft of Sensitive Information and Plaintiff's digital assets if Defendant had remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field.

18. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff is now in imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to dedicate time and resources which they otherwise would have dedicated to other life demands, such as work and family, to mitigate the actual and potential impact of the Data Breach on their life

19. Plaintiff has spent, and will continue to spend, significant amounts of time and money trying to protect themselves from the adverse ramifications of the Data Breach and dealing with actual fraud and will forever be at a heightened risk of identity theft and fraud. Plaintiff has suffered severe financial harm as a direct result of Defendant's reckless disregard for the security of user data.

20. Plaintiff alleges claims for (1) negligence; (2) invasion of privacy; (3) breach of contract/breach of implied covenant of good faith and fair dealing; (4) breach of implied contract; (5) unjust enrichment; (6) breach of fiduciary duty; (7) breach of confidence; (8) gross negligence;

(9) declaratory judgment and injunctive relief; (10) violations of The Washington Consumer Protection Act ("CPA") (RCWA § 19.86.020, *et seq.*); and (11) violations of Washington State Data Breach Notification Law (RCWA § 19.255.010). Plaintiff seeks damages, including but not limited to, recovery of actual damages from Defendant, nominal damages from Defendant, statutory damages, treble damages pursuant to the CPA (RCW § 19.86.090), attorneys' fees and costs from Defendant, and to compel Defendant to adopt reasonably sufficient security practices to safeguard Sensitive Information that remains in Defendant's custody to prevent incidents like the Data Breach from reoccurring in the future.

JURISDICTION AND VENUE

21. This Court has jurisdiction over all causes of action asserted herein pursuant to 28 U.S.C. § 1332(a). The amount in controversy, exclusive of interests and costs, exceeds $75,000, and Plaintiff is a citizen of a different state than Defendant.

22. Plaintiff is a citizen of Washington because their domicile is in Washington.

23. Defendant is a citizen of Massachusetts because its headquarters and principal place of business is located in Massachusetts. Its employees are remote working all across the United States as well as other countries.

24. This Court has personal jurisdiction over Defendant as Defendant has conducted, and continues to conduct, substantial business in Washington and has intentionally availed itself of the laws and markets of Washington through the persistent operation of its business in Washington.[3][4] Additionally, Defendant is a registered business in active status with the Secretary of State in Washington; The registered agent to accept service in Washington is located at the following address: 300 Deschutes Way Southwest, Suite 208 MC-CSC1, Tumwater, WA 98501.

25. Venue is proper in this District pursuant to 28 U.S.C § 1391 because Defendant

[3] Code.org Improved Organizational Security for Password Sharing, Last Pass, (last accessed January 28, 2025), (Citing to a success story of a business client with its primary place of business in Seattle, Washington) https://www.lastpass.com/resources/case-studies/code-org-needed-password-sharing#:~:text=While%20their%20home%20base%20is%20in%20Seattle%2C,workshops%2C%20service%20students%2C%20and%20grow%20the%20organization.

[4] LastPass Password Manager, University of Washington, (last accessed January 28, 2025), (University of Washington approves LastPass Enterprise for UW Employees), https://uwconnect.uw.edu/it?id=kb_article_view&sysparm_article=KB0034324.

purposefully engages in activities in this District, including transacting substantial business in this District and engaging in the acts and omissions alleged herein, in this District.

PARTIES

A. PLAINTIFF

26. Plaintiff is an individual over the age of eighteen years and at all times relevant herein was and is a resident of the County of King in the State of Washington.

27. At all times relevant herein Plaintiff was a subscriber/customer of LastPass. In making the decision to entrust their Sensitive Information to LastPass, Plaintiff relied upon Defendant to safeguard their data.

28. On or about December 21, 2023, Plaintiff created a Ethereum, self-custodian wallet (hereinafter, "E-Wallet"). Plaintiff's E-Wallet was created a Ledger hardware device.

29. When self-custodian wallet is generated, such as Plaintiff's E-Wallet, it provides a seed phrase that can be used to regenerate the wallet in case the devise is lost or damaged.

30. Plaintiff exclusively stored the seed phrase on a LastPass brand password vault to their personal email address.

31. At all times, the Ledge device was in Plaintiff's exclusive possession. The last transaction belonging to Plaintiff on their E-Wallet was on or about December 31, 2023.

32. However, on or about February 19, 2024, for about six (6) minutes, an unknown threat actor began transferring assets from their E-Wallet.

33. Plaintiff had over $200,000 in cryptocurrency assets stolen. This amount excludes estimated loss from change in value and deprivation of use since February 19, 2024.

34. The very next day, Plaintiff filed a police report with the Woodinville Police Department in King County Washington and forwarded the report to the Seattle FBI Cyber Crimes.

35. On or about March 6, 2024, the Woodinville Police Department requested assistance from an FBI agent. It was forwarded to the Cybercrime division.

36. A special agent assigned to the case confirmed a high-level threat actor converted all assets to Bitcoin and parked funds in a Bitcoin address. The threat actor address(es) are unable to be accessed by the FBI and the funds have not been recouped.

37. The Woodinville Police Report notes that it is most likely that the LastPass Data Breach is the manner in which Plaintiff's Sensitive Information was obtained, noting that it appears the only accounts accessed had LastPass associations and other accounts not associated with LastPass protections were not accessed.

38. Plaintiff did not receive notice from Defendant of the related August 2022 and November - December 2022 data breaches.

39. Plaintiff is very careful about sharing their highly sensitive Sensitive Information. The LastPass Data Breach has, through no fault of Plaintiff's own, exposed them to the theft of their cryptocurrency assets.

40. Plaintiff would not have given Defendant their Sensitive Information had they known that the sensitive information collected by Defendant would be at risk of compromise and misuse due to Defendant's negligent data security practices.

41. Plaintiff has suffered the damages described herein, including but not limited to, the fraudulent removal of cryptocurrency from their E-Wallet due to the compromise of their Sensitive Information; the lost value of their privacy; not receiving the benefit of their bargain with Defendant; losing the difference in the value between the services with adequate data security that Defendant promised and the services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their life, including, that required to change multiple account passwords, the master password, monitor accounts, and file police reports and reports with the FBI. Additionally, Plaintiff has been put at increased, substantial risk of future fraud and/or misuse of their Sensitive Information, which may take years to manifest, discover, and detect.

B. DEFENDANT

42. Defendant is a limited partnership incorporated in Massachusetts and has its principal place of business in Boston, Massachusetts. Defendant operates a cloud based secure information storage platform providing password management services nationwide, including to residents of Washington.

43. Defendant, as a password and identity management services company, had access to its users' Sensitive Information and failed to secure the received Sensitive Information or implement any

data security measures sufficient to ensure that the highly sensitive customer data that it stored would be securely handled.

FACTUAL ALLEGATIONS

A. Defendant Acquires, Collects, and Stores Plaintiff's and Consumers' PII

44. Defendant acquires, collects, and stores a massive amount of its consumers' protected confidential information and other personally identifiable data.

45. Specifically, Defendant allows customers to store, control and monitor highly sensitive account passwords, cryptocurrency keys, and other personal account information in their customer vaults, promising to "work[] tirelessly to advance the world of digital security[,]" and "improv[e] the LastPass tools [its] customers know and love to ensur[e] that [its customers'] data belongs only to [them]."[5]

46. Customers, such as Plaintiff, use their vaults to store their Sensitive Information in a safe and encrypted environment so as to protect such Information from unauthorized use, which unauthorized use would lead to the access and misuse of user passwords, cryptocurrency keys, and other personal account information stored in the customer vaults.

47. By requiring, obtaining, collecting, using, and deriving a benefit from Plaintiff's Sensitive Information, Defendant assumed legal and equitable duties, and knew or should have known it was responsible for protecting Plaintiff's Sensitive Information from disclosure.

48. Plaintiff has taken reasonable steps to maintain the confidentiality of their Sensitive Information. Plaintiff relied on Defendant to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, to only allow authorized disclosures of this information, and prevent unauthorized disclosure of the information.

B. The Data Breach

49. On August 25, 2022, LastPass issued the following notice:

> To All LastPass Customers, I want to inform you of a development that we feel is important for us to share with our LastPass business and consumer community. Two weeks ago, we detected some unusual activity within portions of the LastPass development environment. After initiating an immediate investigation, we have seen no evidence that this incident involved any access to customer data or encrypted password vaults. We have determined that

[5] *See* https://www.lastpass.com/company/about-us (last accessed March 14, 2025).

> an unauthorized party gained access to portions of the LastPass development environment through a single compromised developer account and took portions of source code and some proprietary LastPass technical information. Our products and services are operating normally. In response to the incident, we have deployed containment and mitigation measures, and engaged a leading cybersecurity and forensics firm. While our investigation is ongoing, we have achieved a state of containment, implemented additional enhanced security measures, and see no further evidence of unauthorized activity. Based on what we have learned and implemented, we are evaluating further mitigation techniques to strengthen our environment. We have included a brief FAQ below of what we anticipate will be the most pressing initial questions and concerns from you. We will continue to update you with the transparency you deserve. Thank you for your patience, understanding and support. Karim Toubba CEO LastPass.

50. Then, on December 22, 2022, LastPass issued an updated notice announcing that an unknown threat actor accessed a cloud-based storage environment leveraging information obtained from the incident previously disclosed in August of 2022.

51. Upon information and belief, the Data Breach involved the data of millions of LastPass users. Hackers were able to copy highly sensitive information that included names, end-user names, billing addresses, email addresses, telephone numbers, IP addresses from which customers were accessing the LastPass service, and customer vault data where certain unencrypted data was stored, including website usernames and passwords, secure notes, and form-filled data.

52. During the delay between the initial August notice irresponsibly stating that users faced no significant risks and the December notice, the risks and damages to Plaintiff were only increasing. A prompt and proper response from Defendant, including full disclosure to all customers involved in the Data Breach of the extent of the Data Breach and the specific information impacted as a result, as well as the risks users faced, would have mitigated those risks and resulting damages substantially, as users would have been able to change their impacted accounts' usernames and passwords, as well as their LastPass master passwords. Users also could have updated their default password iterations.

53. Therefore, Defendant's disclosure, in addition to being unreasonably delayed, has been woefully inadequate and directly contributed to the damages suffered by Plaintiff thus far, and Defendant has yet to offer any remedy to assist Plaintiff through the devastating aftermath of its Breach. Instead, Defendant took months to "investigate" the ongoing Data Breach. Its investigation is still ongoing and may reveal even more egregious aspects of the Breach than those that have already

been revealed, including, upon information and belief, that LastPass stored users' master password hashes with the usernames, thus allowing hackers to pull the full list of password hashes and start targeting and cracking specifically targeted master passwords.

54. Furthermore, the Data Breach exposed the physical addresses of the customers who lost their information in the Data Breach, meaning that Plaintiff's home billing addresses will not be safe unless they change their address.

55. Defendant not only failed to adequately disclose the Data Breach to Plaintiff, but it also failed to explain the extent of the Data Breach, where the information was lost, to whom it may have been lost, and the extent of exposure of Plaintiff's Sensitive Information.

C. The Value of PII and the Effects of Unauthorized Disclosure

56. Defendant was well aware of the highly private nature of the Sensitive Information it collects and its significant value to those who would use it for wrongful purposes.

57. Sensitive Information is a valuable commodity to identity thieves. As the Federal Trade Commission ("FTC") recognizes, identity thieves can commit an array of crimes including identify theft, medical fraud, and financial fraud.[6] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

58. Preservation of the confidentiality of Sensitive Information is a valuable property right. The value of the Sensitive Information is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences.

59. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[7]

60. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable consequences if its data

[6] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed January 30, 2025).
[7] *See, e.g.*, https://datacoup.com/ (last accessed March 14, 2025).

security systems were breached.

D. Defendant Failed to Comply with Industry Standards

61. Defendant encourages and allows customers to store, control and monitor highly sensitive account passwords, cryptocurrency keys, and other personal account information in their customer vaults, promising that security is its priority and that "customers feel confident using LastPass due to its best-in-class security features that protects accounts and passwords against unauthorized access and data breaches." Defendant promises that LastPass is "trusted by companies and individuals everywhere", that "millions [of] customers secure their passwords with LastPass" and "100,000+ businesses choose LastPass."[8]

62. Customers use their vaults to store their Sensitive Information in a safe and encrypted environment so as to protect such Information from unauthorized use, which unauthorized use would lead to the access and misuse of user passwords, cryptocurrency keys, and other personal account information stored in the customer vaults.

63. As part of its consumer facing business, Defendant offers a universal password manager that allows a user to access password protected accounts across websites with a single master password.[9] Defendant's customer vaults are secured with a master password, where Defendant represents that customers' "data is kept secret, even from us" and the customer LastPass Vaults are "encrypted and decrypted at the device level. Only you can unlock it with your master password."[10]

64. Defendant claims in its blog post that these master passwords were not among the Sensitive Information accessed in the Data Breach, and that they could not have been accessed in the Breach because "the master password is never known to LastPass and is not stored or maintained by LastPass."[11] Defendant goes even further to shift blame and/or cast doubt on LastPass's fault by stating "it would be extremely difficult to attempt to brute force guess master passwords for those customers who follow our password best practices."[12]

[8] LastPass, LastPass Home Page, (January 30, 2025), https://www.lastpass.com/.
[9] *Id.*
[10] LastPass, Why LastPass, (January 30, 2025), https://www.lastpass.com/why-lastpass.
[11] Karim Toubba, *03-01-2023: Security Incident Update and Recommended Actions*, (January 30, 2025), https://blog.lastpass.com/posts/security-incident-update-recommended-actions.
[12] *Id.*

65. However, Defendant never provided direct notice to Plaintiff of any such "best practices," nor did it ever attempt to enforce these practices; not to mention, Defendant's "stronger-than-typical" implementation of 100,100 iterations of the PBKDF2 algorithm (Defendant's password algorithm) is actually well below the standard 310,000 iterations recommendation by the Open Web Application Security Project ("OWASP").[13]

66. Defendant's own notice also fails to rule out the possibility of brute force or other type of attacks against Plaintiff's vault in order to access the Sensitive Information, attacks which would not be possible but for the Data Breach.

67. Defendant's shift of blame on its own customers rather than acknowledge their own data security failures, is misplaced, as they failed to implement any of their own best practices according to industry standards.

68. Defendant's failures, not Plaintiff's, led to the Data Breach and resulting harm now suffered by Plaintiff.

69. Furthermore, because the attackers were also able to compromise websites as a result of the Breach, they can target specific people who have specific accounts – for example, they could target users, like Plaintiff, who have purchased cryptocurrency, making their efforts to break into specifically targeted vaults much more efficient and less time consuming.

70. Many password managers have solved this issue by either adding a truly random factor to the encryption – a secret key – or by switching to key generation methods that are much more difficult to brute force than PBKDF2.[14] Others that similarly use only roughly 100,000 password iterations will also add another 100,000 iterations when their users' respective master passwords are stored on the company's server, thereby totaling roughly 200,000 iterations.[15]

71. Private cybersecurity businesses have also identified it as being particularly vulnerable to cyber-attacks, both because of the value of the PII they maintain and because employees have been slow to adapt and respond to cybersecurity threats.[16] These private cybersecurity firms have also

[13] *See* https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html#pbkdf2 (last accessed April 11, 2025).

[14] *See* https://www.theverge.com/2022/12/28/23529547/lastpass-vault-breach-disclosure-encryption-cybersecurity-rebuttal (last accessed December 29, 2022).

[15] *See Id.*

[16] Stickman Cyber, *Why Cybersecurity In The Workplace Is Everyone's Responsibility, available at:*

promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of PII.

72. Defendant has implemented none of these best practices yet now attempts to blame its customers for its very own data security failures that led to the Data Breach and resulting harms now suffered by Plaintiff.

73. Despite the abundance and availability of information regarding the threats and cybersecurity best practices to defend against those threats, Defendant chose to ignore them. These best practices were known, or should have been known by Defendant, whose failure to heed and properly implement industry standards directly led to the Data Breach and the unlawful exposure of Sensitive Information.

74. Defendant failed to implement several basic cybersecurity safeguards that can be implemented to improve cyber resilience and require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture.

E. Defendant Failed to Comply with FTC Guidelines

75. The FTC promulgates numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

76. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[18] The guidelines note that businesses should protect the personal customer information they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

77. The FTC further recommends companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on

https://www.stickmancyber.com/cybersecurity-blog/why-cybersecurity-in-the-workplace-is-everyones-responsibility (last accessed May 20, 2025).

[17] Federal Trade Commission, *Start With Security*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed January 30, 2025).

[18] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed January 30, 2025).

networks; use industry–tested methods for security; monitor for suspicious activity on the network; and verify third–party service providers have implemented reasonable security measures.[19]

78. The FTC brings enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

79. Defendant was prohibited by the FTCA, 15 U.S.C. § 45 from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

80. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

81. Defendant was aware (or should have been aware), at all times, of its obligation to protect the Sensitive Information of Plaintiff because of its position as possessor and controller of such data. Defendant was also aware (or should have been aware as a password and identity management services company) of the significant repercussions that would result from its failure to do so.

F. Defendant Knew or Should Have Known of the Risk Because Large Entities are Particularly Susceptible to Cyber Attacks

82. As aforementioned, private cybersecurity businesses are particularly vulnerable to cyber-attacks.

83. The number of U.S. data breaches surpassed 1,000 in 2016—a record high and a 40

[19] FTC, *Start With Security*, *supra.*

percent increase in the number of data breaches from the previous year.[20] In 2017, 1,579 breaches were reported—a new record high and a 44.7 percent increase in just one year.[21] That trend continues.

84. Defendant knew and understood that unprotected or exposed Sensitive Information in the custody, possessor, and controller of Sensitive Information, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Sensitive Information through unauthorized access. Indeed, when compromised, highly confidential related data is among the most sensitive and personally consequential. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impacts the economy as a whole.

85. As a private cybersecurity business entrusted with safeguarding the most sensitive, private information of consumers by way of its purported, unbreakable password security, Defendant knew, or should have known, the importance of safeguarding Sensitive Information entrusted to it by Plaintiff, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

G. Plaintiff's Exposure

86. At all relevant times, Defendant understood the Sensitive Information it collects from its users is highly sensitive and of significant property value. Defendant itself uses data value and data privacy as a selling point for its own products.[22]

87. Plaintiff entrusted Defendant in safeguarding their Sensitive Information. Defendant was subject to the Data Breach and failed to notify Plaintiff.

88. The fact that Plaintiff's Sensitive Information was inadvertently disclosed to bad actors that should not have had access to it – and has already been fraudulently misused – demonstrates the monetary value of the Sensitive Information.

[20] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html (last accessed January 30, 2025).

[21] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf (last accessed January 30, 2025).

[22] *See* https://www.lastpass.com/company/about-us ("Doing nothing [to prevent data breaches] could mean losing everything.") (last accessed March 14, 2025).

89. As a direct result of the Data Breach, Plaintiff will continue to be at heightened risk for financial fraud, and identity theft, and the attendant damages, for years to come.

90. The Sensitive Information belonging to Plaintiff is private, sensitive in nature, and left inadequately protected by Defendant—who did not obtain Plaintiff's consent to disclose such Sensitive Information to any other person as required by applicable law and industry standards.

91. Plaintiff is very careful about sharing their highly private Sensitive Information. Even so, Defendant has, through no fault of Plaintiff's own, exposed Plaintiff to the theft of their cryptocurrency assets and exposed them to continued risk.

92. The ramifications of Defendant's failure to keep Plaintiff's Sensitive Information secure are long-lasting and severe. Once that kind of Sensitive Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

93. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems," and that "resolving the problems caused by identity theft may take more than a year for some victims."[23]

94. Plaintiff suffered actual injury from having their Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) theft of cryptocurrency assets that, to this day, are unrecoverable; (b) damages to and diminution in the value of their Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant; (c) loss of their privacy; (d) imminent and impending injury arising from the increased risk of fraud and identity theft; and (e) the time and expense of mitigation efforts as a result of the Data Breach.

95. Had Plaintiff been made aware of Defendant's lax data security practices, unwillingness to promptly and completely disclose data breaches such as this one, failure to provide timely notice and mitigatory assistance, or if Plaintiff knew that Defendant holding their Sensitive Information would be at risk of compromise and subsequent misuse due to Defendant's negligent

[23] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed January 30, 2025).

data security practices, Plaintiff would not have agreed to allow their Sensitive Information to be held by Defendant.

H. Defendant's Delay in Identifying & Reporting the Breach Caused Additional Harm.

96. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[24]

97. Indeed, once a data breach has occurred:

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills, insurance invoices, and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves (internal citations omitted).[25]

98. Although their Sensitive Information was improperly exposed, Plaintiff having not been properly notified of the Data Breach, depriving Plaintiff of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

99. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, there is an increased risk of fraud for Plaintiff.

I. Plaintiff Suffered Damages

100. Plaintiff has suffered damages from the Data Breach as set forth herein.

101. As a result of the Data Breach, Plaintiff's Sensitive Information, which has value in both legitimate and dark markets, has been damaged and diminished by its compromise and

---

[24] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, *available at:* https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed January 30, 2025).

[25] Consumer Reports, *The Data Breach Next Door: Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too*, January 31, 2019, *available at:* https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed January 30, 2025).

unauthorized release. This transfer of value occurred without any consideration paid to Plaintiff for their property.

102. As a direct result from the exposure of Plaintiff's Sensitive Information once entrusted to Defendant to safeguard, Plaintiff lost over $200,000 in cryptocurrency assets. Since the time the cryptocurrency was stolen, Plaintiff also has lost interest that otherwise would have accrued on the amount stolen.

103. Upon information and belief, the Data Breach has also exposed the address(es) of Plaintiff, which inherently impacts their physical security.

104. Knowing that thieves had access to Plaintiff's Sensitive Information, were successful in stealing digital assets as a result, and that Plaintiff's Sensitive Information may now or in the future be available for sale on the dark web, has caused Plaintiff great anxiety. They are now very concerned about fraud and identity theft.

105. As a direct result of the Defendant's failures to prevent the Data Breach, Plaintiff has suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Sensitive Information;

b. Out–of–pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and loss of productivity from addressing and attempting to mitigate actual and future consequences of the Data Breach, including but not limited to researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their Sensitive Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Sensitive Information in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of Plaintiff's life.

106. In addition, Plaintiff has incurred the following types of damages: the lost value of their privacy; not receiving the benefit of their bargain with Defendant; losing the difference in the value between the services with adequate data security that Defendant promised and the services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their life, including, *inter alia*, that required to change multiple account passwords, the master password, monitor accounts, and file police reports and reports with the FBI. Additionally, Plaintiff has been put at increased, substantial risk of future fraud and/or misuse of their Sensitive Information, which may take years to manifest, discover, and detect.

107. In addition to a remedy for the economic harm, Plaintiff maintains an undeniable interest in ensuring their Sensitive Information is secure, remains secure, and is not subject to further misappropriation and theft.

First Cause of Action

Negligence

108. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

109. Defendant's own negligent conduct created a foreseeable risk of harm to Plaintiff. Defendant's negligence included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's negligence also included its decision not to comply with (1) industry standards, and/or best practices for the safekeeping and encrypted authorized disclosure of the Sensitive Information of Plaintiff; or (2) Section 5 of the FTCA.

110. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing its security protocols to ensure Sensitive Information in Defendant's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on relevant cybersecurity measures. Defendant also had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiff's Sensitive Information.

111. As promised by Defendant, Plaintiff their Sensitive Information to Defendant with the understanding that Defendant would safeguard their information.

112. Defendant was in a position to protect against the harm suffered by Plaintiff as a result of the Data Breach. However, Plaintiff had no ability to protect their Sensitive Information in Defendant's possession.

113. Defendant had full knowledge of the sensitivity of the Sensitive Information, and the types of harm Plaintiff could, would, and will suffer when the Sensitive Information was wrongfully disclosed.

114. Plaintiff was the foreseeable and probable victim of Defendant's negligent and inadequate security practices and procedures that led to the Data Breach. Defendant knew or should have known of the inherent risks in collecting and storing the highly valuable Sensitive Information of Plaintiff, the critical importance of providing adequate security of that Sensitive Information, the current cyber security risks being perpetrated, and that Defendant had inadequate IT security systems, employee training, monitoring, and education and IT security protocols in place to secure the Sensitive Information of Plaintiff.

115. Defendant negligently, through its actions and/or omissions, and unlawfully breached its duty to Plaintiff by failing to exercise reasonable care in protecting and safeguarding Plaintiff's Sensitive Information while the data was within Defendant's possession and/or control by failing to comply with and/or deviating from standard industry rules, regulations, and practices at the time of the Data Breach.

116. The harm the Data Breach caused is the type of harm privacy laws were intended to guard against. Plaintiff is within the class of persons privacy laws were intended to protect.

117. Defendant negligently failed to comply with privacy laws by failing to protect against and prevent the dissemination of Plaintiff's Sensitive Information to unauthorized third parties.

118. Defendant's violations of Section 5 of the FTC Act also constitute negligence. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Sensitive Information. The FTC publications and

orders described above also form part of the basis of Defendant's duty in this regard.

119. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's Sensitive Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information it required, obtained, and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff.

120. Plaintiff is within the class of persons the FTC Act was intended to protect.

121. The harm the Data Breach caused, and continues to cause, is the type of harm the FTC Act was intended to guard against. The FTC pursues enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff.

122. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of Plaintiff's Sensitive Information.

123. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff the existence and scope of the Data Breach.

124. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff, Plaintiff's Sensitive Information would not have been compromised.

125. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the Sensitive Information and the harm suffered, and/or risk of imminent harm suffered, by Plaintiff.

126. As a direct and proximate result of Defendant's negligence, Plaintiff has suffered, and continue to suffer, injuries and damages arising from the Data Breach, including, but not limited to: damages from lost time and efforts to mitigate the actual and potential impact of the Data Breach on their life, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, reporting theft to numerous authorities, damages from cryptocurrency assets and

appreciation of said assets over the years, communicating with the FBI, and damages from identity theft, which may take months—if not years—to discover, detect, and remedy.

127. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff has suffered, and will continue to suffer, the continued risks of exposure of their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession.

Second Cause of Action

Invasion of Privacy

128. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

129. Plaintiff had a legitimate expectation of privacy with respect to their Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

130. Defendant owed a duty to its customers, including Plaintiff, to keep their Sensitive Information confidential.

131. The unauthorized release of Sensitive Information, especially social security numbers, addresses, and driver's license numbers, is highly offensive to a reasonable person.

132. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff entrusted Defendant with safeguarding their Sensitive Information as an integral part and promise of Defendant's business, but privately, with the intention that the Sensitive Information would be kept confidential and protected from unauthorized disclosure. Plaintiff was reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

133. The Data Breach constitutes an intentional interference with Plaintiff's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

134. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

135. Acting with knowledge, Defendant had notice and knew its inadequate cybersecurity practices would cause injury to Plaintiff.

136. As a proximate result of Defendant's acts and omissions, Plaintiff's Sensitive Information was disclosed to, and used by, third parties without authorization, causing Plaintiff to suffer damages.

137. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff in that the Sensitive Information maintained by Defendant may be breached again, leading to further viewing, distributing, and use of updated and additional Sensitive Information by unauthorized persons.

138. Plaintiff has no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff.

Third Cause of Action

Breach of Contract/Breach of Implied Covenant of Good Faith and Fair Dealing

139. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

140. Plaintiff entered into a valid and enforceable express contract with Defendant under which Plaintiff agreed to provide their Sensitive Information to Defendant, and Defendant agreed to provide password and identity management services that included the implementation of adequate data security standards, protocols, and procedures to ensure the protection of Plaintiff's Sensitive Information.

141. In the contract entered into between Plaintiff and Defendant, there is an implied covenant of good faith and fair dealing obligating the parties to refrain from unfairly interfering with the rights of the other party or parties to receive the benefits of the contracts. This covenant of good faith and fair dealing is applicable here as Defendant was obligated to protect (and not interfere with) the privacy and protection of Plaintiff's Sensitive Information.

142. To the extent Defendant's obligation to protect Plaintiff's Sensitive Information was not explicit in its express contract, the contract also included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's Sensitive Information, including in accordance with trade regulations, federal, state and local laws, and industry standards. Plaintiff would not have entered into this contract with Defendant without the understanding that their Sensitive Information would be safeguarded and protected; stated otherwise, data security was an essential term of the parties' express contract.

143. Indeed, Section 4.2 of Defendant's Terms of Service for Personal Users states that LastPass "ha[s] implemented and maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure."

144. Plaintiff agreed, among other things, to provide their Sensitive Information in exchange for Defendant's agreement to protect the confidentiality of that Sensitive Information.

145. The protection of Plaintiff's Sensitive Information was a material aspect of Plaintiff's contract with Defendant.

146. Defendant's promises and representations described above relating to industry standards and Defendant's purported concern about its users' privacy rights are express terms of the contract between Defendant and Plaintiff. Defendant breached these promises by failing to comply with reasonable industry practices.

147. Plaintiff read, reviewed, and/or relied on statements made by or provided by Defendant and/or otherwise understood that Defendant would protect its customers' Sensitive Information if that information was provided to Defendant.

148. Plaintiff fully performed their obligations under their contract with Defendant; however, Defendant did not.

149. As a result of Defendant's breach of these terms, Plaintiff has suffered a variety of damages including but not limited to: actual damage of stolen cryptocurrency assets and the ongoing lost difference in interest value from the time of the theft to present; the lost value of their privacy; not receiving the benefit of their bargain with Defendant; losing the difference in the value

between the services *with* adequate data security that Defendant promised and the services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their life, including, *inter alia*, that required to change multiple account passwords, the master password, monitor accounts, and file police reports and reports with the FBI. Additionally, Plaintiff has been put at increased risk of future fraud and/or misuse of their Sensitive Information, which may take years to manifest, discover, and detect.

150. Plaintiff is therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

Fourth Cause of Action

Breach of Implied Contract

151. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

152. Plaintiff brings this claim alternatively to their claim for breach of contract.

153. Through its course of conduct, Defendant entered into an implied contract with Plaintiff for the provision of password and identity management services, as well as implied contracts for Defendant to implement data security practices adequate to safeguard and protect the privacy of Plaintiff's Sensitive Information.

154. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when they first began using Defendant's services.

155. The valid and enforceable implied contract to provide password and identity management services that Plaintiff entered into with Defendant include Defendant's promise to protect nonpublic Sensitive Information entrusted to it.

156. When Plaintiff provided their Sensitive Information to Defendant in exchange for Defendant's services, they entered into an implied contract with Defendant pursuant to which Defendant agreed to reasonably protect such information.

157. Defendant solicited and invited Plaintiff to provide their Sensitive Information as part of Defendant's regular business practices. Plaintiff accepted Defendant's offer and provided their Sensitive Information to Defendant.

158. By entering into such implied contract, Plaintiff reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

159. Under the implied contract, Defendant promised and was obligated to: (a) provide password and identity management services to Plaintiff; and (b) protect Plaintiff's Sensitive Information provided to obtain such benefits of such services. In exchange, Plaintiff agreed to turn over their Sensitive Information to Defendant.

160. Both the provision of password and identity management services and the protection of Plaintiff's Sensitive Information were material aspects of the implied contract.

161. The implied contract for the provision of password and identity management services, including but not limited to, the maintenance of the privacy of Plaintiff's Sensitive Information, are also acknowledged, memorialized, and embodied in Defendant's Terms of Service for personal users.

162. Defendant's express representations, including, but not limited to, the express representations found in its Terms of Service, memorialize and embody the implied contractual obligations requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff, and to protect the privacy of Plaintiff's Sensitive Information.

163. Users of password management services value their privacy and the ability to keep their Sensitive Information associated with obtaining such services. Plaintiff would not have entrusted their Sensitive Information to Defendant and entered into this implied contract with Defendant without an understanding that their Sensitive Information would be safeguarded and protected; nor would they have entrusted their Sensitive Information to Defendant in the absence of the implied promise by Defendant to monitor the Sensitive Information and to ensure that it adopted reasonable administrative and data security measures.

164. A meeting of the minds occurred, as Plaintiff agreed and provided their Sensitive Information to Defendant in exchange for, among other things, both the provision of password management services and the protection of their Sensitive Information.

165. Plaintiff performed their obligations under the contract when they turned over their Sensitive Information to Defendant.

166. Defendant promised to comply with privacy standards, and to make sure Plaintiff's Sensitive Information would remain protected.

167. Implicit in the agreement between Plaintiff and Defendant, regarding providing protected Sensitive Information, was Defendant's obligation to: (a) use such Sensitive Information for business purposes only; (b) take reasonable steps to safeguard that Sensitive Information; (c) prevent unauthorized disclosures of the Sensitive Information; (d) provide Plaintiff with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information; (e) reasonably safeguard and protect the Sensitive Information of Plaintiff from unauthorized disclosure or uses; and (f) retain the Sensitive Information only under conditions that kept such information secure and confidential.

168. Defendant breached the implied contract with Plaintiff by failing to:

a. Reasonably safeguard and protect Plaintiff's Sensitive Information, which was compromised as a result of the Data Breach; and,

b. Identify and respond to suspected or known security incidents.

169. Defendant materially breached its contractual obligation to protect the nonpublic Sensitive Information it gathered when the Sensitive Information was compromised and subsequently misused as a result of the Data Breach.

170. Defendant materially breached the terms of this implied contract, including, but not limited to, the terms stated in the relevant Terms of Service. Defendant did not maintain the privacy of Plaintiff's Sensitive Information as evidenced by its notices of the Data Breach posted on its blog. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA or otherwise protect Plaintiff's Sensitive Information as set forth above.

171. The Data Breach was a reasonably foreseeable consequence of Defendant's data security failures in breach of the implied contract.

172. As a result of Defendant's failure to fulfill the data security protections promised in the contract, Plaintiff did not receive the full benefit of their bargain with Defendant and instead received services that were of a diminished value to that described in the contract. Plaintiff therefore was damaged in an amount at least equal to the difference in the value of the password management accounts with data security protection that Defendant agreed to provide and the services Defendant actually provided.

173. Without such implied contract, Plaintiff would not have provided their Sensitive Information to Defendant. Had Defendant disclosed that its administrative and data security measures were inadequate or that it did not adhere to industry-standard security measures, neither Plaintiff, nor any reasonable person, would have utilized services from Defendant.

174. As a direct and proximate result of the Data Breach, Plaintiff was harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation, lost cryptocurrency assets, interest on lost cryptocurrency assets, the release and disclosure of their Sensitive Information, the loss of control of their Sensitive Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their life, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months if not years to discover, detect, and remedy, and the loss of the benefit of the bargain they struck with Defendant.

175. Plaintiff is entitled to compensatory and consequential damages suffered as a result of the Data Breach.

176. Plaintiff is also entitled to injunctive relief requiring Defendant to, e.g., strengthen its data security systems and monitoring procedures, and immediately provide adequate credit monitoring to Plaintiff.

Fifth Cause of Action

Unjust Enrichment

177. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

178. Plaintiff conferred a monetary benefit on Defendant.

179. Specifically, they provided Defendant with their Sensitive Information. In exchange, Plaintiff should have received from Defendant the services that were the subject of the transaction and were entitled to have Defendant protect their Sensitive Information with adequate data security.

180. Defendant knew and appreciated that Plaintiff conferred a benefit on it and accepted and retained that benefit. Defendant profited from Plaintiff's providing of their Sensitive Information to it for business purposes.

181. Defendant failed to secure Plaintiff's Sensitive Information and, therefore, did not provide full compensation for the benefit that Plaintiff's Sensitive Information provided.

182. Defendant acquired the Sensitive Information through inequitable means as it failed to disclose the inadequate security practices alleged herein.

183. If Plaintiff knew that Defendant did not have data security safeguards in place that were adequate to secure their Sensitive Information from unauthorized access, they would not have used Defendant's services.

184. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff conferred upon it.

185. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff, proceeds in the amount of the benefits that it unjustly received from them by way of possessing and controlling Plaintiff's Sensitive Information.

186. This claim is being asserted in the alternative to Plaintiff's claims for breach of contract.

Sixth Cause of Action

Breach of Fiduciary Duty

187. Plaintiff re-alleges and incorporates by reference each and every allegation contained

in the preceding and subsequent paragraphs as though fully set forth herein.

188. In light of their special relationship, Defendant became the guardian of Plaintiff's Sensitive Information. Defendant became a fiduciary, created by its undertaking and guardianship of Plaintiff's Sensitive Information, to act primarily for the benefit of Plaintiff. This duty included the obligation to safeguard Plaintiff's Sensitive Information, and to timely notify them in the event of a data breach.

189. Defendant has a fiduciary duty to act for the benefit of Plaintiff upon matters within the scope of its relationship. Defendant breached its fiduciary duties owed to Plaintiff by failing to:

a. Properly encrypt and otherwise protect the integrity of the system containing Plaintiff's protected confidential information and other Sensitive Information;

b. Timely notify and/or warn Plaintiff of the Data Breach; and

c. Otherwise failing to safeguard Plaintiff's Sensitive Information.

190. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff has suffered, and will suffer, injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity to control how their Sensitive Information is used; (c) the compromise, publication, and/or theft of their Sensitive Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Sensitive Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect its customers' Sensitive Information in continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of Plaintiff's life.

191. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff has suffered, and will continue to suffer, other forms of injury and/or harm, and other economic and non–economic losses.

Seventh Cause of Action

Breach of Confidence

192. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

193. At all times during Plaintiff's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's Sensitive Information that Plaintiff provided to Defendant.

194. As alleged herein and above, Defendant's relationship with Plaintiff was governed by terms and expectations that Plaintiff's Sensitive Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

195. Plaintiff provided their respective Sensitive Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Sensitive Information to be disseminated to any unauthorized parties.

196. Plaintiff also provided their Sensitive Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Sensitive Information from unauthorized disclosure, such as following basic principles of protecting its networks and data systems, including Defendant's employees' systems.

197. Defendant required and voluntarily received, in confidence, Plaintiff's Sensitive Information with the understanding that the Sensitive Information would not be disclosed or disseminated to the public or any unauthorized third parties.

198. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's Sensitive Information, Plaintiff's Sensitive Information was disclosed to, and misappropriated by, unauthorized third parties beyond Plaintiff's confidence, and without their express permission.

199. As a direct and proximate result of Defendant's actions and/or omissions, Plaintiff has suffered, and will continue to suffer damages.

200. But for Defendant's disclosure of Plaintiff's Sensitive Information in violation of the parties' understanding of confidence, Plaintiff's Sensitive Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's Sensitive Information, as well as the resulting damages.

201. The injury and harm Plaintiff suffered, and continue to suffer, was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's Sensitive Information. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's Sensitive Information had numerous security and other vulnerabilities placing Plaintiff's Sensitive Information in jeopardy.

202. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff has suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their Sensitive Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of Plaintiff's life; and (g) the diminished value of Defendant's services they received.

203. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff has suffered and will continue to suffer other forms of injury and/or harm, and other economic and non–economic losses.

Eighth Cause of Action

Gross Negligence

204. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

205. Upon Defendant's acceptance and storage of Plaintiff's Sensitive Information in its system, Defendant undertook and owed a duty to Plaintiff to exercise reasonable care to secure and safeguard that Information and to use commercially reasonable methods to do so. Defendant knew that Plaintiff's Sensitive Information was highly sensitive and confidential and should be protected as such.

206. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described herein, but also because Defendant was bound by industry standards to do more to protect the confidential data that was compromised as a result of the Data Breach.

207. Defendant owed a duty of care not to subject Plaintiff's Sensitive Information to an unreasonable risk of exposure and theft because Plaintiff was a foreseeable and probable victim of any inadequate data security practices.

208. The numerous duties Defendant owed to Plaintiff, included at least the following: to exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting Sensitive Information in its possession; to protect Sensitive Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and to implement processes to quickly detect a data breach and to timely act on warnings about data breach. Defendant's duty of care to use reasonable data security measures arose as a result of the special relationship that existed between Defendant and Plaintiff, which is recognized by laws and regulations, including but not limited to, common law. Defendant was in a position to ensure that its systems and protocols were sufficient to protect against the foreseeable risk of harm to Plaintiff from the compromise of the data with which it was entrusted.

209. Defendant knew, or should have known, of the risks inherent in collecting and storing Plaintiff's Information and the importance of adequate data security.

210. Defendant knew, or should have known, that its data systems and privacy protocols and procedures would not adequately safeguard Plaintiff's Sensitive Information.

211. Defendant breached its duties to Plaintiff by failing to provide fair, reasonable, or adequate computer systems, networks, and/or data security practices to safeguard Plaintiff's Sensitive Information, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Sensitive Information. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Sensitive Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of compromise and misuse, which permitted malicious bad actors to gather Plaintiff's Sensitive Information and intentionally disclose it to others and/or misuse it without consent, resulting in the harms alleged herein

212. Defendant's own conduct created a foreseeable risk of harm to Plaintiff their Sensitive Information. Defendant's misconduct included failing to (1) secure Plaintiff's Sensitive Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; (4) implement the systems, policies, and procedures necessary to prevent the Data Breach; and, (5) wholly failing to provide timely notice to Plaintiff of the Data Breach so that they could take appropriate steps to mitigate the potential for fraud, theft, and other damages.

213. Through Defendant's acts and omissions described in this Complaint, including its failure to provide notice and adequate data security and protect Plaintiff's Sensitive Information from being foreseeably accessed, stolen, disseminated, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's Sensitive Information during the time it was within Defendant's possession and control.

214. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to, failing to adequately protect the Sensitive Information, and failing to provide Plaintiff with timely notice that their Sensitive Information had been compromised.

215. In no way did Plaintiff contribute to the Data Breach and subsequent misuse of their Sensitive Information as described in this Complaint. Any and all actions taken by Plaintiff which

Defendant may argue contributed to the misuse of the compromised Sensitive Information were reasonable under the circumstances.

216. As a direct and proximate result of Defendant's conduct, Plaintiff suffered damages as alleged herein.

217. Plaintiff is also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; and (ii) submit to future audits of those systems and monitoring procedures.

Ninth Cause of Action

Declaratory Judgment and Injunctive Relief

218. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

219. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the regulations described in this Complaint.

220. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective duties to reasonably safeguard users' Sensitive Information and whether Defendant is maintaining data security measures adequate to protect Plaintiff from further data breaches that compromise their Sensitive Information, including but not limited to, their respective customer vaults.

221. Plaintiff alleges that Defendant's data-security measures remain inadequate. Defendant denies these allegations and goes so far as to attempt to cast the blame of the harm suffered by Plaintiff upon Plaintiff. In addition, Plaintiff continues to suffer injury as a result of the compromise of their Sensitive Information and remain at imminent risk that further compromises of their Sensitive Information and continued fraudulent activity against them will occur in the future.

222. Pursuant to its authority under the Declaratory Judgment Act, Plaintiff asks the Court to enter a judgment declaring, among other things, the following: (i) LastPass owes a duty to secure consumers' Sensitive Information and to timely notify consumers of a data breach under the

common law, Section 5 of the FTC Act, and various state statutes; and (ii) LastPass is in breach of these legal duties by failing to employ reasonable measures to secure consumers' Sensitive Information in its possession and control.

223. Plaintiff further asks the Court to issue corresponding prospective injunctive relief requiring Defendant, LastPass, to employ adequate security protocols consistent with law and industry standards to protect consumers' Sensitive Information from future data breaches.

224. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at LastPass. The risk of another such breach is real, immediate, and substantial. If another breach at LastPass occurs, the Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and Plaintiff will be forced to bring multiple lawsuits to rectify the same misconduct.

225. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to LastPass if an injunction is issued. Among other things, if a similar data breach occurs again due to the repeated misconduct of LastPass, Plaintiff will likely be subjected to substantial hacking and phishing attempts and other damage, in addition to the damages already suffered. On the other hand, the cost to LastPass of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and LastPass has pre-existing legal obligations to employ such measures.

226. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing additional data breaches at LastPass, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose personal and confidential information would be further compromised.

Tenth Cause of Action

Violation of the Washington Consumer Protection Act,

RCW § 19.86.020, *et seq*.--Unfair Business Practices

227. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

228. Defendant violated RCW § 19.86.020, *et seq*. (hereinafter, "CPA"), by engaging in

unlawful, unfair, or deceptive acts and practices in the conduct of trade or commerce.

229. Defendant is a corporation organized and operated for profit or financial benefit of its owners. Specifically, Defendant is a large, global password and identity management company that collects consumers' Sensitive Information as an integral component to effectuating its services in trade or commerce. It urges consumers to trust their "pioneer" expertise in safeguarding personal data in the rise of data breaches.

230. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect consumers', such as Plaintiff's, Sensitive Information. As detailed herein, Defendant failed to do so.

231. Moreover, Defendant misled the public into believing its security practices, the heart of Defendant's business, were robust and trustworthy.

232. Defendant engaged in unfair, deceptive acts and practices by: establishing the sub–standard security practices and procedures described herein; by soliciting and collecting Plaintiff's Sensitive Information with knowledge, or at least reckless disregard, that the information would not be adequately protected; and by storing Plaintiff's Sensitive Information in an unsecure electronic environment; by victim-blaming customers, like Plaintiff, for failing to follow "best practices" when Defendant itself fails to adhere to baseline industry standards; and, by failing to disclose the Data Breach in a timely and accurate manner.

233. The Data Breach had an immense impact on the public interest. Defendant's services are utilized by millions of users and over 100,000 businesses worldwide. Considering Defendant has shifted blame to its consumers, rather than admit to and provide notice for its security shortcomings and Data Breach, there is grave potential the same misconduct and deceptive practice would reoccur. The primary purpose of Defendant's business, safeguarding the Sensitive Information of consumers, was compromised and misused, which undoubtedly undermines consumers' confidence.

234. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's Sensitive Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above–named unlawful

practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff.

235. As a direct and proximate result of Defendant's unlawful and unfair practices and acts, Plaintiff was injured and lost money and property, including but not limited to the loss of Plaintiff's cryptocurrency digital assets, their legally protected interest in the confidentiality and privacy of their Sensitive Information, nominal damages, and additional losses as described herein.

Eleventh Cause of Action

Violation of Washington State Data Breach Notification Law

RCWA § 19.255

236. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

237. Subsection 1 of the RCWA 19.255.010 requires any "person or business that conducts business in [Washington], and that owns or licenses computerized data that includes personal information [to] disclose any breach of the security of the system to any resident of [Washington] whose personal information was, or is reasonably believed, to have been, acquired by an unauthorized person and the personal information was not secured." It further requires "[t]he breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person."

238. In subsection 2, the RCWA further provides: "Any person or business that maintains or possess data that includes personal information that the person or business does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

239. Pursuant to subsection 6 of the RCWA 19.255.010, any person or business required to issue a security breach notification shall meet the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following

information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. A time frame of exposure, if known, including the date of breach and date of discovery of the breach; and,

iv. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information

240. As set forth herein, Defendant is a business that owns or licences data, or at the very least, maintains or possesses data including personal information for the purposes of RCWA 19.255.010.

241. The Data Breach described herein constituted a "breach of the secured personal information" of Plaintiff whereby the Sensitive Information acquired and accessed was either "not secured during a security breach" or the "confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person."

242. Defendant failed to disclose to Plaintiff,

243. Defendant violated RCWA 19.255.010 by failing to disclose the Data Breach to Plaintiff, an affected Washington resident, without unreasonable delay, not to exceed thirty (30) days, when Defendant knew or reasonably believed Plaintiff's Sensitive Information had been compromised.

244. The delay in notification contributed to the harm and damages suffered by the Plaintiff as described herein.

245. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

246. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff would impede its investigation.

247. As a result of Defendant's violation of RCWA § 19.255.010, Plaintiff was deprived of prompt notice of the Data Breach, and was thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff because their stolen information would have had less value to identity thieves.

248. As a result of Defendant's violation of RCWA § 19.255.010, Plaintiff suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

249. Plaintiff seeks all remedies available including, but not limited to, the damages suffered by Plaintiff as alleged above and equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

1. Granting injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff, including but not limited to an order:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein,

   ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws,

   iii. requiring Defendant to delete, destroy, and purge the personal information of Plaintiff unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff,

   iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal information of Plaintiff's personal information,

   v. prohibiting Defendant from maintaining Plaintiff's personal information on a

cloud-based database,

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors,

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring,

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures,

ix. requiring Defendant to conduct regular database scanning and securing checks,

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal information, as well as protecting the personal information of Plaintiff,

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,

xii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal information,

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor

Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated,

xiv. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected,

xv. requiring Defendant to disclose any future data disclosures in a timely and accurate manner; and

xvi. requiring Defendant to provide ongoing credit monitoring and identity theft repair services.

2. An award of compensatory, statutory, treble, and nominal damages in an amount to be determined;

3. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

4. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

5. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all claims so triable.

DATED: May 22, 2025

SWIGART LAW GROUP, APC

/s/ Joshua B. Swigart
Joshua B. Swigart
Attorneys for Plaintiff